March [insert], 2016

[FName] [LName]
[Address1] [Address 2]
[City], [State] [Zip]
Group #1

Re: Notice of Data Breach

Dear [FName]:

We are sending this letter to you to inform you that we take your privacy very seriously, and it is important to us that you are fully aware of the potential privacy issue that recently arose.

What Happened and What Information Was Involved?

On Friday, March 11, 2016, certain personal information of current and former employees of ARC International North America, LLC, Cardinal International III, LLC and Durand Glass Manufacturing Company, LLC (collectively "ARC") was mistakenly transmitted by ARC via email to a third party posing as an officer of ARC. In particular, the personal information was transmitted as part of (i) an Excel spreadsheet file that comprised the name, address, city, state, zip code, date of birth, job title and annual base compensation amount of current employees, and (ii) PDF files containing the copies of W-2 forms for those persons who were ARC employees at any time during 2015. Those W-2 form copies included the name, address, city, state, zip code, Social Security number, gross compensation amount, federal income tax withholding amount, Social Security wage and tax withholding amounts, Medicare wage and tax withholding amounts, gross state compensation amount, and state income tax withholding amount (and comparable local tax information) of each such person. In your situation, your information was included on both of these files transmitted. In addition, please note that no insurance, health/medical, banking, or other information was involved in this matter. ARC learned of this situation shortly after the transmission occurred. We have contacted the New Jersey State Police to report the matter and they are investigating now. We are also taking numerous steps to make sure that such a transmission does not happen again.

What ARC is Doing

We truly regret that this breach has occurred and apologize for any difficulty or inconvenience it may cause you. In this regard, we have conducted several in-person meetings with employees on the date of the discovery, and over the past several days to advise them of this situation and have transmitted email notices about this situation to those persons for whom we have email addresses.

What You Can Do

We are keenly aware of how important your personal information is to you. To protect yourself from potential harm resulting from the breach we encourage you to closely monitor all mail or other contact from individuals not known to you personally, and avoid answering any questions or providing additional information to those individuals.

As an added precaution, at our expense, we are providing a service to you that can help protect you against misuse of this information. We are offering a complimentary two-year membership of Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. Since we are not authorized to enroll you in this program, we strongly encourage you to take the necessary steps to enroll, as outlined below:

Activate ProtectMyID Elite Now in Three Easy Steps:

1. **Visit the ProtectMyID Web Site**: http://www.protectmyid.com/enroll , or call 877-441-6943 to enroll (and provide engagement Number PC 100042)
2. **PROVIDE** Your Activation Code: **[Insert code]** :
3. **ENSURE that you enroll by: June 30, 2016 (your code will not work after this date)**

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
  - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
  - **Change of Address:** Alerts of any changes in your mailing address.
- **Identity Theft Resolution & ProtectMyID:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - **ExtendCARE**: It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance**[1] Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-441-6943.

In addition to registering for the service provided to you, the Federal Trade Commission suggests the following steps if you believe your identity has been stolen or may be stolen:

1. Place a fraud alert on your credit reports and review your credit reports. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two companies.

    a. ***Equifax***. 1-800-525-6285. P.O. Box 740241, Atlanta, GA 30374-0241. www.equifax.com ;

    b. ***Experian***. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9532, Allen, TX 75013. www.experian.com ;

    c. ***TransUnion***. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790. www.transunion.com .

    Once you place the fraud alert, you are entitled to order free copies of your credit reports.

2. Carefully review your credit reports. Look for inquiries from companies that you haven't contacted, accounts that you did not open, and debts on your accounts that you can't explain. Be aware that some companies may bill under names other than their store names.

3. Close any accounts that you know, or believe, have been tampered with or opened fraudulently.

4. File your concern(s) with the Federal Trade Commission. This important information helps law enforcement agencies track down identity thieves. You can contact the Federal Trade Commission by calling 1-877-ID-THEFT (1-877-438-4338), or by visiting the Federal Trade Commission website at www.ftc.gov/idtheft , or writing to the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

5. File a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year.

Other Information

Finally, you can request that a security freeze be placed on your credit file by contacting each of the three reporting agencies listed above and/or contacting the Federal Trade Commission to receive additional information regarding security freezes. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a security freeze in place, even you will need to take special steps when you wish to apply for any type of credit. Please note, because of more stringent security features, you will need to place a security freeze separately with each of the three major credit reporting companies if you want the freeze on all of your credit files. A security freeze remains on your credit file until you remove it or choose to lift it temporarily when applying for credit or credit-dependent services. When requesting a security freeze, be prepared to provide your name, address, social security number, and date of birth.

In addition to the foregoing actions, we also recommend that you complete IRS Form 14039 as soon as possible to advise the IRS of the compromise to your personal information. It is available for download at the IRS website www.irs.gov; Hardcopies of this form are also available to you through your local Human Resources Department. Once received, this form will enable the IRS to flag your tax file so as to examine any returns that it subsequently receives to be sure that they are truly from you. If you have additional questions, you may call the IRS Identity Protection Specialist Unit at 1-800-908-4490.

Maryland Residents: Please note, you can reach the Maryland Attorney General at 1-888-743-0023 (toll-free) to receive further information on steps you can take to avoid identity theft.

For More Information

If you have any questions or need any help with anything mentioned in this letter, please contact me by e-mail at stephanie.ojeda@arc-intl.com or by phone at (609)501-6431 (m), or (856)825-5620 ext. 3502(o). In addition, if you believe that your information has been used without your authorization, please notify your local law enforcement officials to enable them to promptly investigate the matter.

We take the responsibility to maintain the security of your information seriously. Please accept our sincere apology for this incident and know that we are taking additional steps, including internal procedural changes, additional training, and other actions necessary to identify any further steps needed to assist us going forward to reduce the risk of this situation recurring.

Sincerely,

Stephanie Ojeda
VP Human Resources
ARC